

Design Methods for Fault Prevention and Fault Management

Irem Y. Tumer, Ph.D.

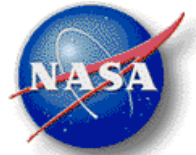
Itumer@mail.arc.nasa.gov

650-604 2976

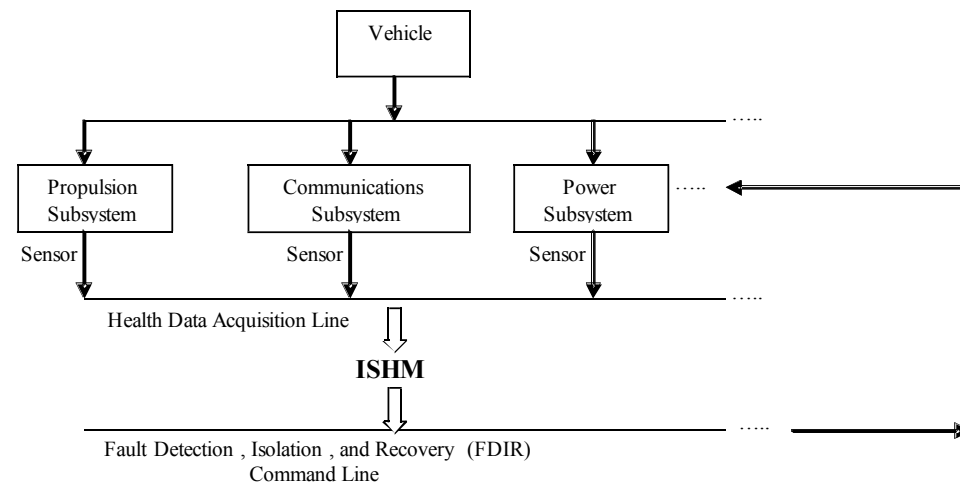
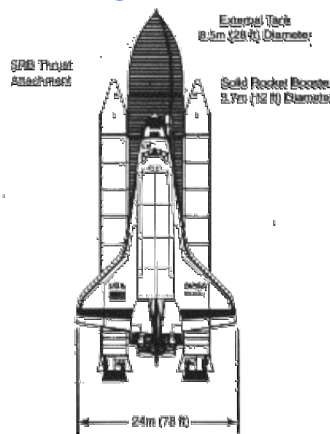
Complex System Design & Engineering Group
Discovery and Systems Health Technical Area
Intelligent Systems Division
NASA Ames Research Center



The ISHM Design Challenge for Exploration Missions

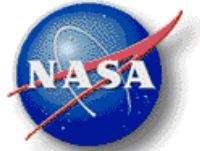


- The art and science of managing off-nominal conditions systems may encounter during their operational life, either by designing out failures early on, or designing in the capability to safeguard against or mitigate failures
- Key enabler for crew autonomy and self-sufficient mission ops
- ISHM has been around in many forms, but to this day, true ISHM has never been achieved
- Key limitation: ISHM/IVHM typically retrofitted as an after-thought, and is typically limited to subsystems
- ESMD Challenge: ISHM must be part of the overall design process and viewed as a system engineering discipline encompassing a variety of technologies & methods





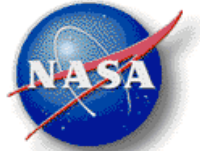
Facing the Challenge of ISHM Design



- Desired:
 - Early influence on system design by ISHM
 - Guide the choice of whether to eliminate failure by design (through part selection and built-in redundancy), by prognosis leading to preventative maintenance, or by fault management (by diagnosis & recovery)
 - Failure modes & effects analysis activities
 - Feed fault information into the design process to create simulations of faults and improved designs to deal with faults
 - The initial design must be examined in the context of the full system life cycle
 - Include all stakeholders (ops, maintenance, etc.) in the design
 - Solution optimized in terms of well-defined Figures of Merit (FOMs)



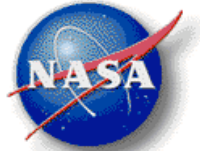
Facing the Challenge of ISHM Design



- Reality:
 - Little interaction during the design process between failure analysis activities and design processes to prevent or mitigate these failures
 - Little interaction between reliability analyses and design processes
 - Little interaction between operational training simulations and assessments of operational dependability and design process
 - Operations and maintenance costs and risks become much larger than initially projected during Phase A initial design
 - No formal tools and methodologies to allow program managers and lower level designers to formulate a clear understanding of the impact of the decisions in the downstream phases such as operations and maintenance on the systems design, and vice versa



ISHM Design Goal

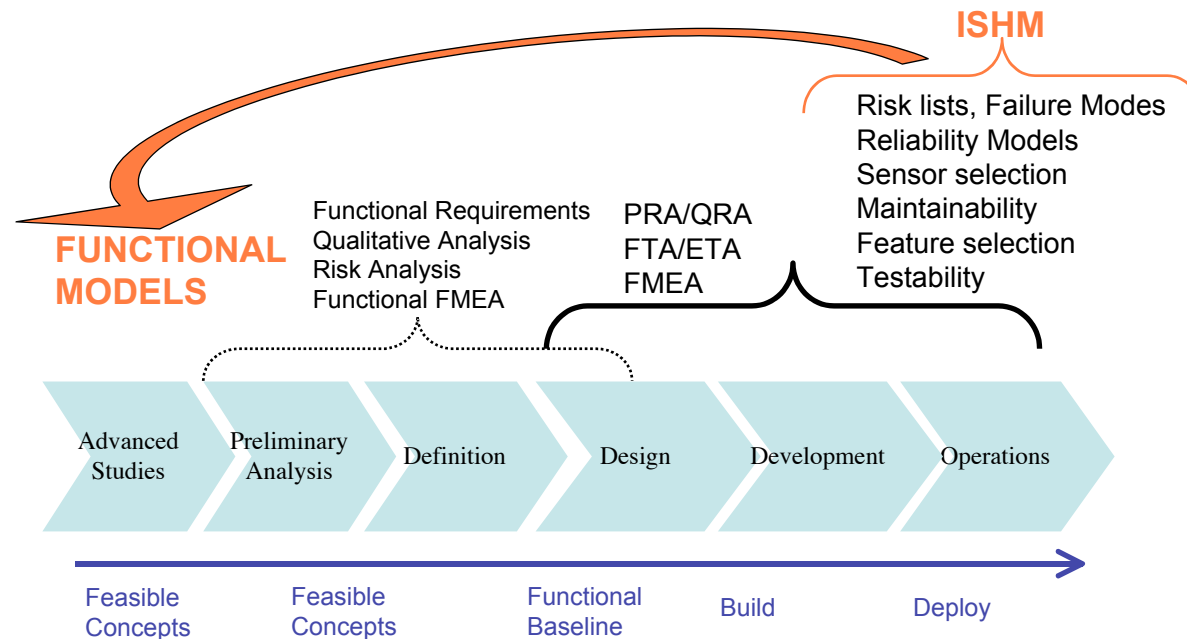
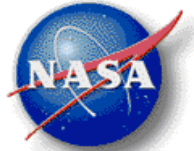


“DESIGN IN” THE ISHM CAPABILITY FROM THE BEGINNING!

- Good news: Current interest is strong!
 - JSF (see Andy Hess keynote)
 - AFRL Design Study (see Mark Derriso, et al.)
 - CEV/CLV
- Bad news: We lack methodologies & tools to achieve this!
- Some successful attempts:
 - Requirements: Specify ISHM “shall” statements at the beginning of project
 - Joint Strike Fighter (5% of requirements are HM related)
 - Boeing 777
 - CEV and CLV
 - Trade Studies: Integrate ISHM design with system-level design and do trade studies with ISHM as a design attribute
 - Northrop/NASA ARC SA&O effort for 2nd Gen RLV program
 - Honeywell/QSI SA&O and modeling effort
 - Integrate operations and maintenance considerations into design:
 - Boeing 777
 - Lessons learned from OSP, B2 bomber...

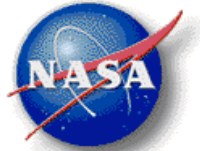


The ISHM Design Paradigm: *Changing the Way ISHM Design is Done*



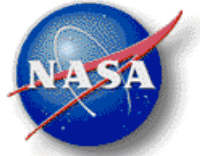
Proposed Design Paradigm Shift #1: Integrate ISHM in the very early functional design stage (including failure and reliability analyses)

Proposed Design Paradigm Shift #2: Assess impact of ISHM FOMs on the system level FOMs (including all stakeholders in the mission lifecycle--design, maintenance, operations)



Key Challenges

- Embedding ISHM design into the early stages of functional design requires high-level modeling and analyses
 - At the early stage, the system's functional requirements may be firm but selection of specific components to implement functionality has not been made, and hence models of system components and design parameters are not yet available
 - In order to integrate the health management of these various systems, a modeling paradigm that is capable of representing the desired functionality of the individual systems as well as their interactions is required
- Failure analyses, reliability and risk analyses must be done at the functional design stage
 - Need mathematical techniques for risk assessment and resource allocation under uncertainty must be incorporated with high-level analyses
- Design of ISHM is multidisciplinary and multiobjective by nature
 - Need mathematical framework to achieve effective analysis & optimization
 - Designing an ISHM that encompasses all subsystems of a space mission is the result of interaction among engineers and managers from different disciplines with their own domain expertise

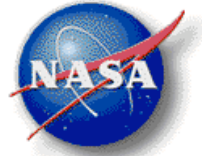


Candidate Design Methods

- Risk and Reliability Based Design Methods (see previous talks)
 - PRA, FTA, FMEA/FMECA, reliability block diagrams, event sequence diagrams, safety factors, knowledge-based methods, expert elicitation
- Design for Testability Methods (see previous talks)
- Formal design theory and methodology (see ASME Design Conferences)
 - High-level modeling techniques:
 - **Function-based design and modeling**
 - Mathematical techniques:
 - Uncertainty modeling, decision-based design, **risk-based design, design optimization**, etc.
 - Systematic methodologies for **Design for X**:
 - Design for ISHM, Design for maintainability, Design for failure prevention
- Focus on three R&D efforts in the CSDE group:
 - Function-based modeling and failure analysis
 - Risk assessment by portfolio management and optimization
 - Multiobjective and multidisciplinary system analysis & optimization



Function-Based Design, Modeling & Failure Modes Analysis



- **Using Function-based design and modeling for ISHM design**
 - Addressing the challenge of assessing failures during early design stages (“functional design”)
 - Designers always think in terms of functionality at the early stages, before a form or solution has been selected and decisions have been finalized
 - Failure analysis typically done once solutions are selected (later in design)
 - Experience has shown that early design is the best stage to catch most failures and mishaps
 - Develop a “Functional Model” to represent ISHM systems
 - A standardized method for representing the functionality of a system, and the interfaces between them
 - A systematic and formal means to represent a complex system early in the conceptual design process, before components have been selected
 - A means to enable the storage and retrieval of design knowledge based on common functionality
 - Correlate historical and potential failure modes with functionality



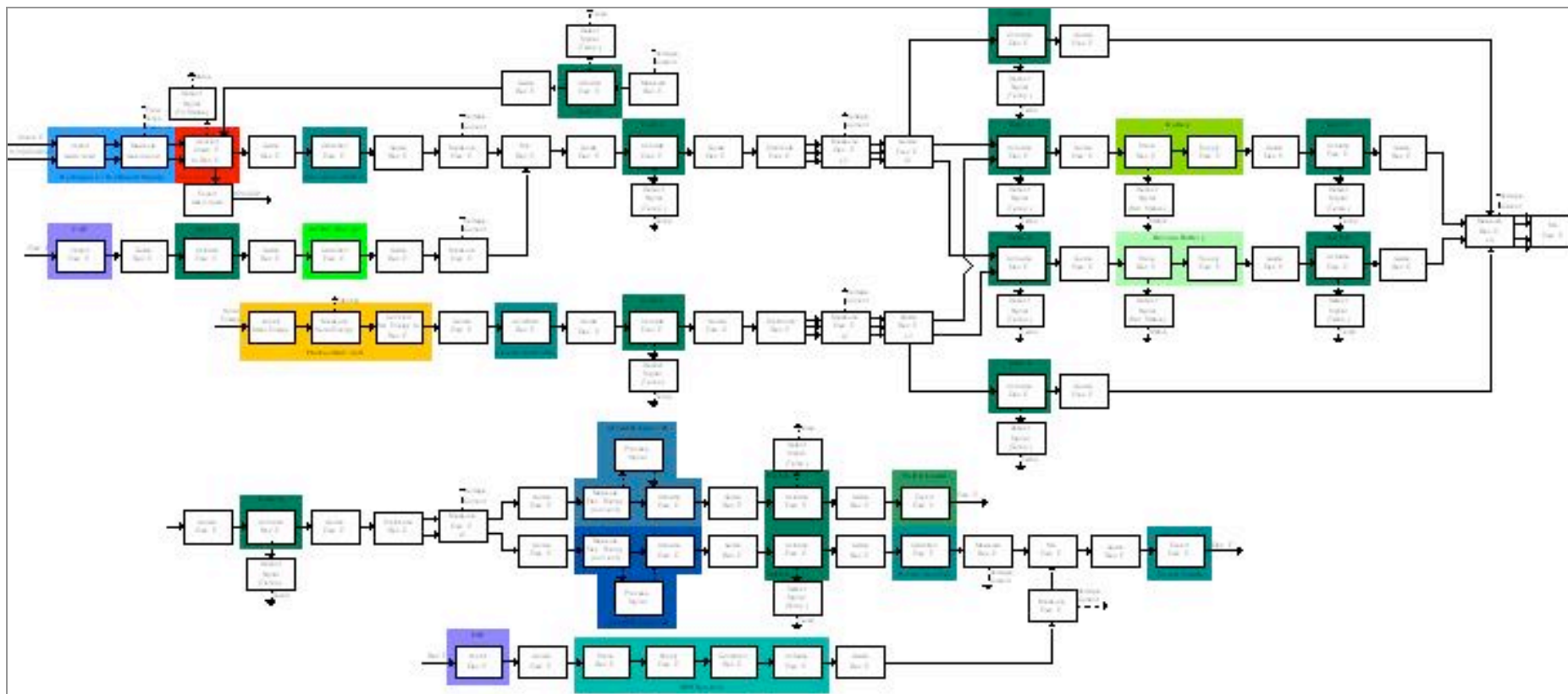
Functional Model: The “Blueprint” of ISHM System

Ex: Functional design of the ADAPT testbed at NASA ARC

Used to discover interfaces and interactions between functions

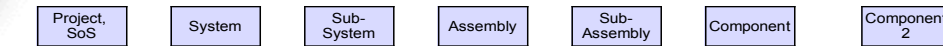
Used to add required functionality for ISHM (detect, sense, activate, etc.)

Used to discover functional failures and add safeguards

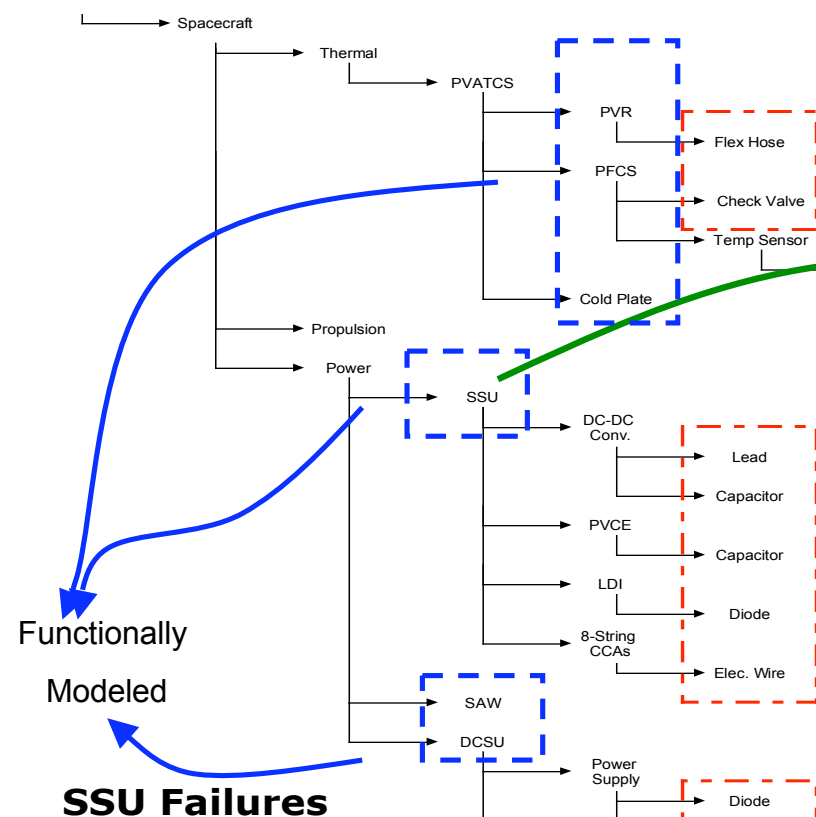




Function-Based Failure Modes Analysis



ISS

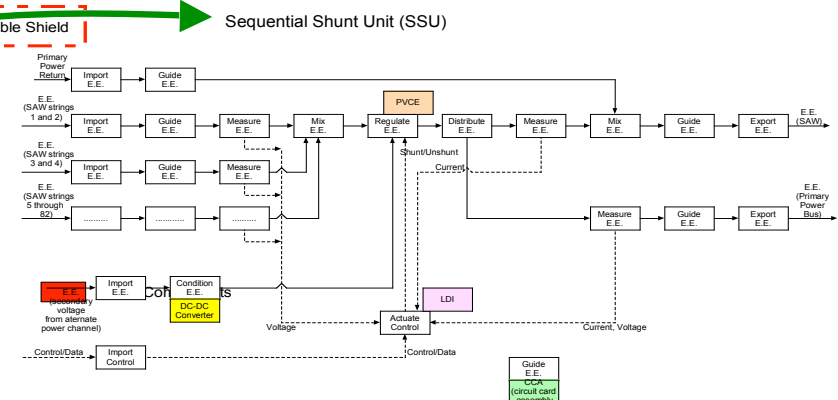


Functionally
Modeled

SSU Failures

Failure Mode	Primary Identifier	Component	Subfunction	Flow	Sub-assembly
Arc Discharge	Breakdown	electric wire	Guide	electrical	8-String CCAs
	Breakdown	diode	Guide/Stop	electrical	LDI
Abrasive Wear	Wear	lead	Guide	electrical	DC-DC Converter
Arc Discharge	Breakdown	capacitor	Store/Supply	electrical	DC-DC Converter
Electrical Overstress	Overstress	capacitor	Store/Supply	electrical	PVCE

- Developing templates for functional models
- Generating database of functions for S/C
- Mining Failure Databases
- Developing a Software Query Interface



Components in colored boxes have failures identified from reports


FFMEA Design Interface (w/ UMR)

Browse Repository

http://module.basiceng.umn.edu:8080/view/browse.jsp

Public x500 Salon News Traffic Processing Java Postgres IEEE PDF eXpress games from sjc to hi

Browse Repository

UMR  **Design Engineering Lab & NASA Ames Research Center**
ARTIFACT BROWSE

Home Browse Artifacts Search Design Tools Dictionary Account Information Online Manual Log Out

- ISS
 - Spacecraft
 - ACS
 - Power
 - Direct Current Switching Unit
 - Sequential Shunt Unit
 - Thermal
 - MER
 - Project-SoS
 - Spacecraft
 - ACS 1
 - ACS 2
 - ACS 3
 - C and DH
 - Computers
 - EDL
 - Instruments
 - Power**
 - Propulsion
 - Science
 - Structures
 - Telecom
 - Thermal
 - team x
 - template

System: Project-SoS

Artifact Name	power	Artifact Photo	no image available	
Part Family	not specified			
Part Number	3			
Sub Artifact Of	spacecraft			
Quantity	1			
Description	not specified			
Artifact Color	not specified			
Component Naming	not specified			

Input Artifact	Input Flow	Subfunction	Output Flow	Output Artifact
external	electrical energy	import	electrical energy	external
external	chemical energy	import	chemical energy	external
external	radioactive nuclear energy	import	radioactive nuclear energy	external
external	electromagnetic energy	import	electromagnetic energy	external
external	electrical energy	regulate	electrical energy	external
external	chemical energy	convert	electrical energy	external
external	electromagnetic energy	convert	electrical energy	external
external	radioactive nuclear energy	convert	electrical energy	external
external	electrical energy	change	electrical energy	external
external	electrical energy	actuate	electrical energy	external
external	electrical energy	mix	electrical energy	external
external	electrical energy	distribute	electrical energy	external
external	electrical energy	store	electrical energy	external
external	electrical energy	supply	electrical energy	external
external	electrical energy	export	electrical energy	external
external	radioactive nuclear energy	export	radioactive nuclear energy	external
external	thermal energy	export	thermal energy	external

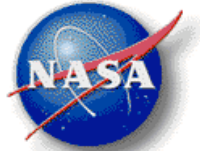
Supporting Functions
there are no supporting functions defined for this artifact.

Physical Parameters no parameters specified	Manufacturing Process material not specified no process specified
---	--

Primary Identifier no primary identifier specified	Failure Mode no failure mode specified
--	--



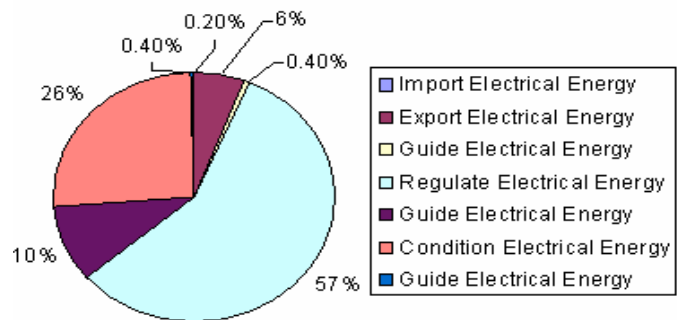
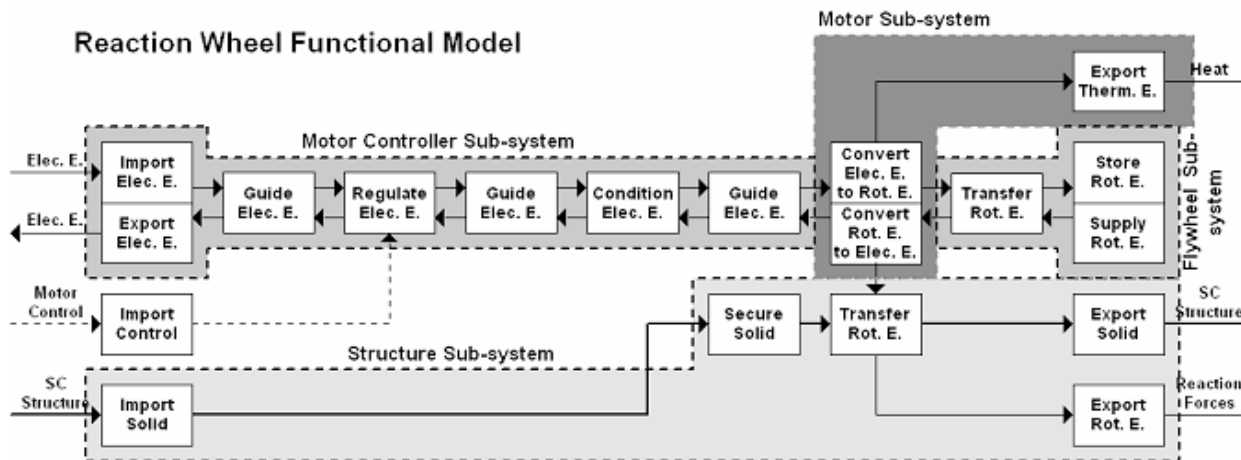
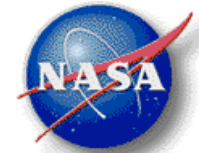
Resource allocation to minimize risks due to functional failures



- **Use of formal risk-based design and optimization techniques for ISHM risk assessment**
 - Risk-informed trade study framework to account for risk & uncertainty in early design: RUBIC design
 - Framework for quantifying risk due functional failures and allocating resources for risk reduction during concurrent design
 - Starting from the functional model, RUBIC optimally allocates resources to mitigate risks due to functional failures
 - Ex of resources: hours spent on analysis, redesign, dollars allocated, acquiring more reliable components, adding redundancy, etc.



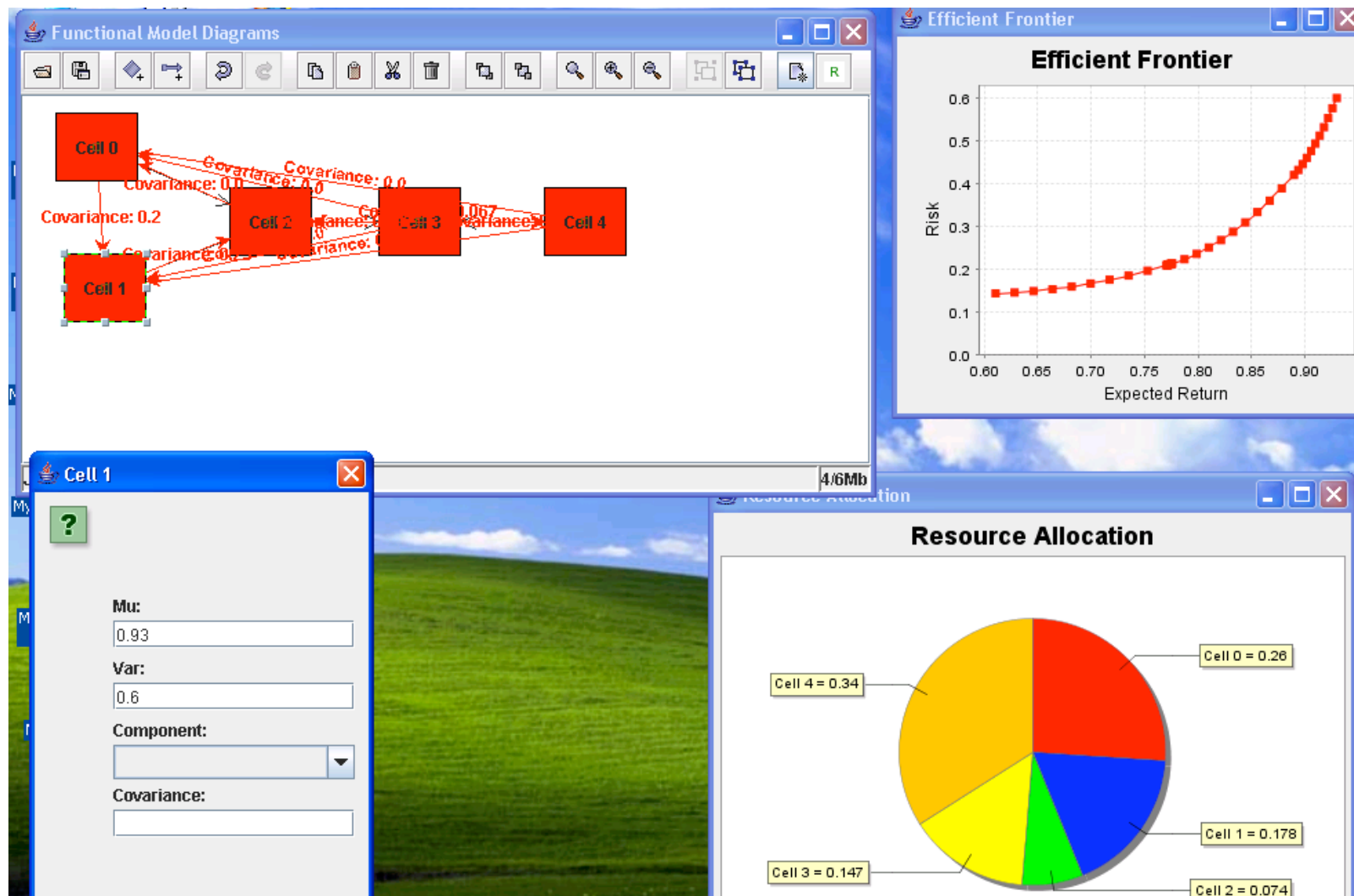
Resource Reallocation to Minimize Risk and Uncertainty due Functional Failures



Column #	Subsystem	Function	Resource Allocation
1 st	Motor Controller	Import Electrical Energy	<<1%
2 nd	Motor Controller	Export Electrical Energy	4%
3 rd	Motor Controller	Guide Electrical Energy	<<1%
4 th	Motor Controller	Regulate Electrical Energy	36%
5 th	Motor Controller	Guide Electrical Energy	6%
6 th	Motor Controller	Condition Electrical Energy	17%
7 th	Motor Controller	Guide Electrical Energy	<<1%
Total Allocation to Controller Subsystem: 64%			
8 th	Motor Controller	Convert Electrical E. to Rotational E.	9%
2 nd	Motor Controller	Convert Rotational E. to Electrical E.	13%
3 rd	Motor Controller	Export Thermal Energy	10%

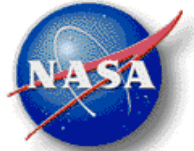


RUBIC Software Prototype Development

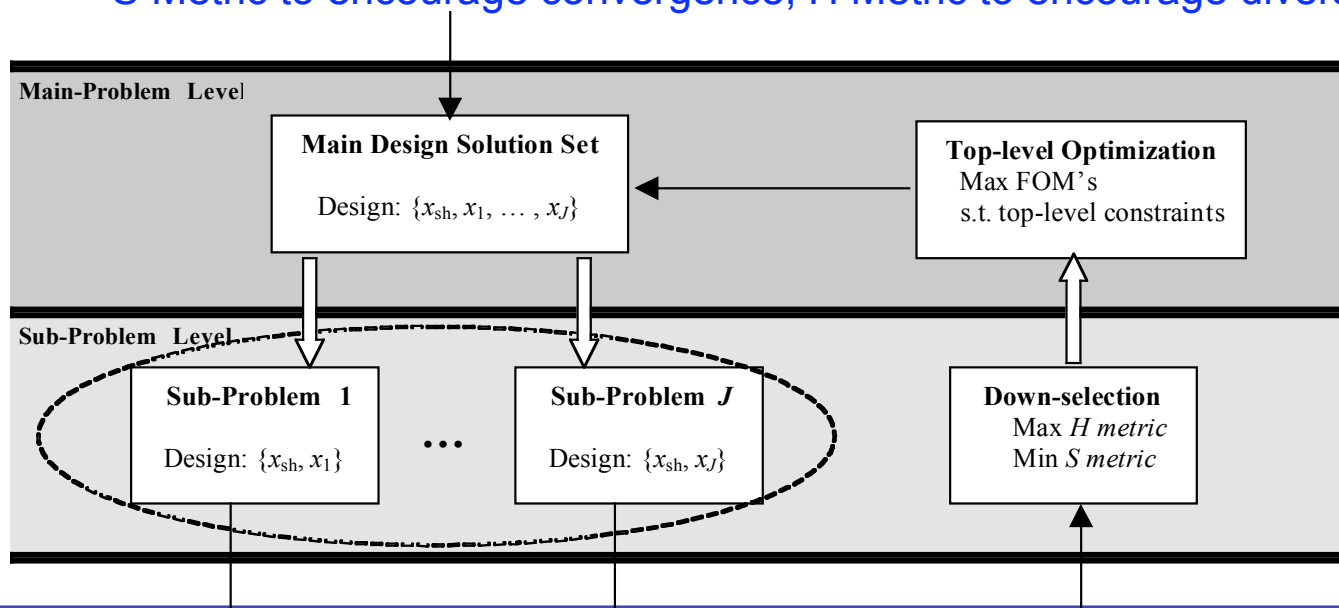




Multi-Disciplinary, Multi-Objective Optimization for ISHM Design

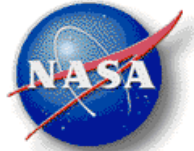


- **Using formal design optimization methods for ISHM**
 - ISHM design can be formulated as an optimization problem
 - ISHM Design Variables
 - ISHM Objectives (Figures of Merit)
 - ISHM Design Constraints: Feasibility Constraints + Hard Requirements
 - Multi-objectives/constraints in each sub-system
 - Functionally separable $F_{i,j}$ and exclusive f_j
 - S Metric to encourage convergence; H Metric to encourage diversity

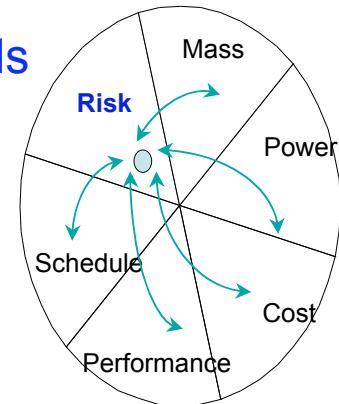




System Analysis & Optimization (SA&O)



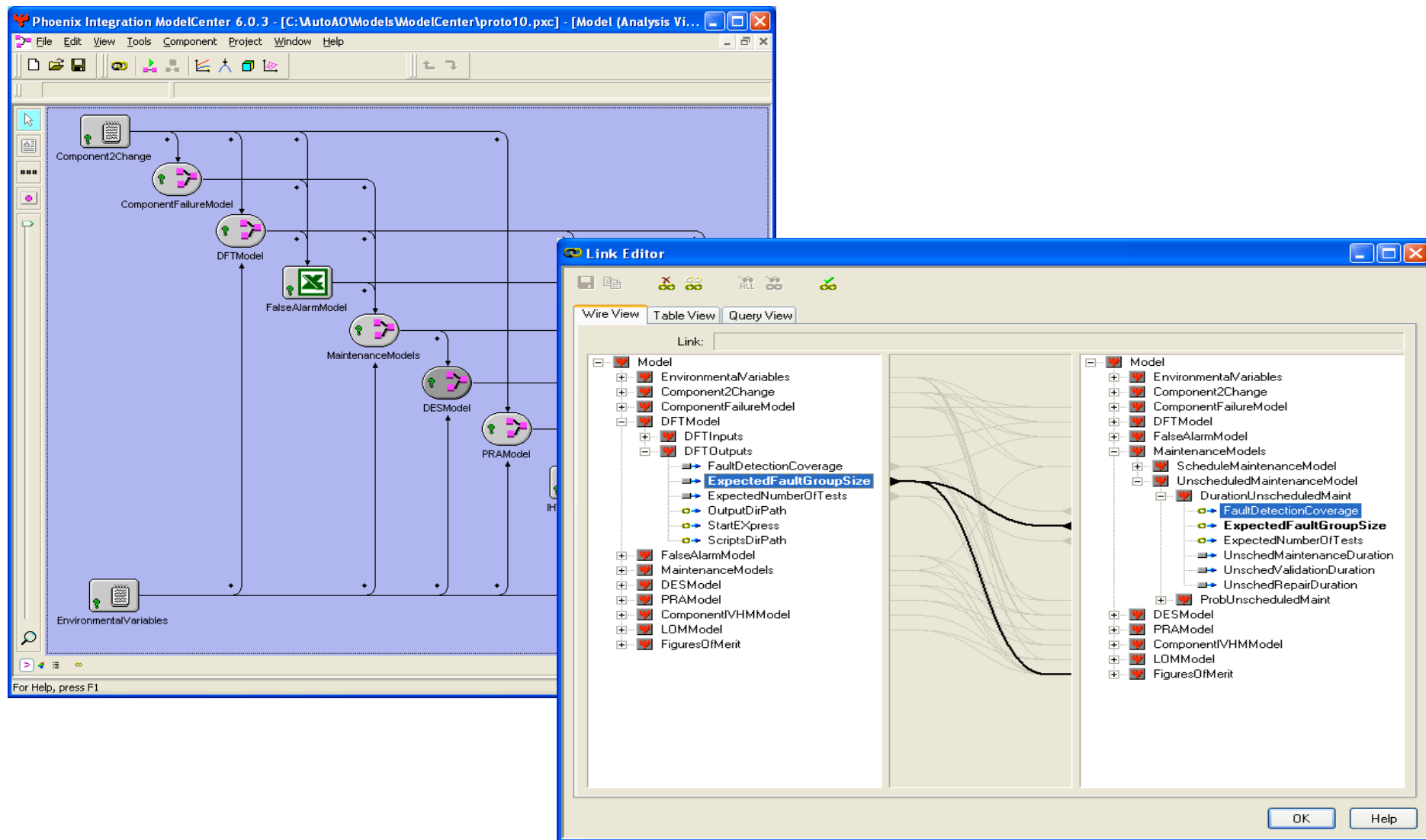
- SA&O Framework (based on prior work done for 2nd Gen RLV by Koushik Dutta and Dougal MacLise):
 - Select a set of Figures-of-Merit
 - Select a set of models such as cost, safety, operations, reliability, false alarm rates and maintainability that generate the FOM
 - Determine the tools to implement the models
 - Determine the data flow requirements between the models
 - Perform trade studies
- Current Enhancements:
 - **Multi-objective & multi-disciplinary optimization**
 - **Data flow/exchange environment** (implemented in Model Center)
 - **Automation for rapid trade analyses**
 - Ability to feed back into functional design stage:
 - Add new functionality to enable ISHM to operate as an integrated system?
 - Change functionality to enable maintainability, performance, reduce risk?





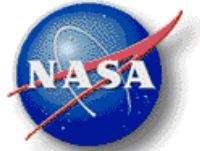
ISHM System Analysis & Optimization

ModelCenter Screenshot





Summary



- Key Message:
 - **Design paradigm shift required for successful ISHM and a sustainable exploration mission**
- Formal Methods & Tools:
 - Reliability based methods, Design for testability tools
 - Function-based design methods to integrate with early design
 - Multiobjective & multidisciplinary optimization for trade studies, SA&O
 - Systematic integrated (Design for ISHM) methodology to co-design ISHM and vehicle systems
- Complex System Design & Engineering Group Capabilities:
 - Function based failure modes analysis
 - Risk and uncertainty based design
 - ISHM system analysis and optimization
- Current Involvement:
 - CEV, CLV for Constellation/ESMD
 - IVHM and Aging Aircraft for Aviation Safety/ARMD